



Virginia Information Technologies Agency



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 21, 2008





Memorial 's Day



May Flowers





ISOAG May 2008 Agenda

- | | | |
|-------|---|---|
| I. | Welcome and Opening Remarks | Peggy Ward, (VITA) |
| II. | ISACA Certifications and Training | Kenneth Magee, (Auditor of Public Accounts) |
| III. | IS ² Certifications and Training | Lynn McNulty, (IS ²) |
| IV. | SANS Certifications and Training | Jeff Pike, (SANS Institute) |
| V. | Division of the State Internal Auditor Training Opportunities | Jack Spooner, (State Internal Auditor) |
| VI. | Altiris Security Controls – Panel Discussion | Don Kendrick, Rodney Caudle, Tony Shoot,
(COV IT Infrastructure Partnership) |
| VII. | IT System Security Guideline | Cathie Brown, (VITA) |
| VIII. | Encrypting Email | Michael Watson, (VITA) |
| IX. | Upcoming Events & Other Business | Peggy Ward, (VITA) |



ISACA ®

Serving IT Governance Professionals.

ISACA ® Certifications

CISA®

CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM®

CERTIFIED INFORMATION
SECURITY MANAGER®

CGEIT™

CERTIFIED IN THE GOVERNANCE
OF ENTERPRISE IT™

ISACA ® Facts

- Founded in 1969 as the EDP Auditors Association
- More than 65,000 members in over 140 countries
- More than 175 chapters in over 70 countries worldwide





ANSI Accreditation

- The American National Standards Institute (ANSI) has awarded accreditation under ISO/IEC 17024 to the Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certification programs. ANSI reaccredited these ISACA programs in 2007.
- Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process.



The Certified Information Systems Auditor (CISA) is ISACA's cornerstone certification. The CISA certification has been earned by more than 55,000 professionals since inception and is for the IS audit, control, assurance and/or security professionals who wish to set themselves apart from their peers. Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

CISA Certification Details

- More than 55,000 CISAs worldwide
- The CISA exam is offered in 11 languages and at over 240 locations
- Certification Magazine's 2007 salary survey ranked CISA in the top five highest paying certifications.
- I'll give you the top five (5) cert's on the last slide



CISA Job Practice Areas

Effective 2007

- 1. IS Audit Process – 10%*
- 2. IT Governance – 15%*
- 3. Systems and Infrastructure Lifecycle Management – 16%*
- 4. IT Service Delivery and Support – 14%*
- 5. Protection of Information Assets – 31%*
- 6. Business Continuity and Disaster Recovery – 14%*



CISA Certification Requirements

- Earn a passing score on the CISA Exam
- Have a minimum of five years of verifiable IS audit, control or security experience (substitutions available)
- Submit the CISA application and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Abide by *IS Auditing Standards* as adopted by ISACA
- Comply with continuing professional education policy



The Certified Information Security Manager (CISM) certification is a unique management focused certification that has been earned by over 7,000 professionals since its introduction in 2003. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise's information security program. CISM defines the core competencies and international performance standards that those who have information security management responsibilities must master.



CISM Certification Current Facts

- More than 7,000 CISM's worldwide
- The CISM exam is offered in 4 languages (English, Japanese, Korean and Spanish) in over 240 locations
- Certification Magazine's 2007 salary survey ranked both CISA and CISM certifications in the top five highest paying certifications
- I'll give you the top five (5) cert's on the last slide



CISM Job Practice Effective June 2007

1. *Information Security Governance (23%)*
2. *Information Risk Management (22%)*
3. *Information Security Program
Development (17%)*
4. *Information Security Program
Management (24%)*
5. *Incident Management and Response
(14%)*



CISM Certification Requirements

- Earn a passing score on the CISM exam
- Submit verified evidence of a minimum of five years of information security work experience
- Submit the CISM application and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Comply with the *CISM Continuing Professional Education Policy*



The IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by a "job practice" consisting of IT governance related tasks and knowledge. Earning this designation will enable professionals to respond to the growing business demand for a comprehensive IT governance program that defines responsibility and accountability across the entire enterprise.



CGEIT Certification Current Facts

- It's new
- The CGEIT exam is offered December 2008 for the first time.
- It hasn't been ranked by Certification Magazine
- You can apply to be “grandfathered” in through October 2008



CGEIT Job Practice

Job Practice: A job practice serves as the basis for the exam and the experience requirements to earn the CGEIT certification. Each job practice consists of task and knowledge statements, organized by domains and are intended to depict the tasks performed by individuals who have a significant management, advisory, or assurance role relating to the governance of IT and the knowledge required to perform these tasks. The domains are as follows:

1. IT Governance Framework (required)
2. Strategic Alignment
3. Value Delivery
4. Risk Management
5. Resource Management
6. Performance Measurement

What does it cost?

- **What is the registration deadline of the next exam and what are the fees?**
- **On or before 20 August 2008**
ISACA member US \$375
Nonmember US \$505
- **After 20 August through 24 September 2008**
ISACA member US \$425
Nonmember US \$555
- **Test Date is 13 December 2008**

Training Events

- Annual ISACA VA Chapter training week on such topics as:
 - Penetration Testing (2 days) by CanAudit
 - CobiT Foundations (2 days) by ITPreneurs
 - Web Security (3 days) by MIS TI
 - Auditing IT (1 day) by CanAudit
 - SOX for Auditors (2 days) by MIS TI
 - Auditing Mobile Workforce (1/2 day) by CyberEnsure

Training Events

- Semi-Annual CISA & CISM review courses
 - May 10th & May 11th (yes it's a weekend)
- Monthly luncheons 3rd Tuesday at “The Place in Innsbrook” guest speakers – 1 CPE
- Monthly e-symposium's – 3 CPEs
- Monthly CPE Quiz in the ISACA Control Journal – 1 CPE

ISACA-VA Chapter Contact Information

Blake Bialkowski, CISA

Director of Certification Program, ISACA-VA Chapter

Information Systems Development Senior Specialist

Auditor of Public Accounts

Phone: (804) 225-3350

Fax: (804) 225-3357

I promised you the top 5 cert's

- #1 at \$117,110 in annual salary – BCSM (Brocade Certified SAN Manager)
- #2 at \$115,720 in annual salary – CISM
- #3 at \$111,090 in annual salary – CCIE (Cisco Certified Internetwork Expert)
- #4 at \$109,510 in annual salary – BCSD (Brocade Certified SAN Designer)
- #5 at \$98,740 in annual salary - CISA



CEH LPT CCSA CWNP
SSCP SABSA
PCIP CIA CSA
CISM SCSE MCSE
SECURITY+ GPMC
CISSP SCSP CGEIT
GCIH ITIL AISC
CSP GLEG
GLDR CISA CFE
ABCP CCIP
ECSA ISSEP CPP
CBCP CCNP CHFI
GIAC ISSAP GSLC
MBCP CCDP GWAS
ISSPCS IAM SSEC
GSAE ISSMP CITP GSNA
IEM GSE
G7799

QUESTIONS

(ISC) 2 OVERVIEW

Lynn McNulty

Director of Government Affairs

May21, 2008

Lynn.McNulty@verizon.net

www.isc2.org



SECURITY TRANSCENDS TECHNOLOGYSM

Outline of Presentation

- Background of (ISC)²
- Review of (ISC)² certifications and concentrations
- Quick look at the current status of the Information Security profession



Speaker Bio—Lynn McNulty

- Retired from Federal Government in 1995 as the Associate Director for Computer Security NIST
 - Worked in the IT security field at CIA, FAA and State
- Served as Director of Government Affairs for RSA Security 1997-2000
- Currently Director of Government Affairs for (ISC)2
- Member of the Information Systems Security and Privacy Advisory Board
- Member of the Executive Committee of the IT Sector Coordinating Committee



Who We Are

- **Established in 1989 - Non-profit consortium of industry leaders**
- **Global leaders in certifying and educating information security professionals throughout their careers**
- **Offer the first information technology-related credentials to be accredited to ANSI/ISO/IEC Standard 17024**
- **Global standard for information security – (ISC)² CBK[®], a compendium of information security topics**
- **Board of Directors -- Top information security professionals worldwide**
- **Nearly 60,000 certified professionals in 135 countries**
- **Produce the only Global Information Security Workforce Study**



Credential Offerings



ISO/IEC 17024



ISO/IEC 17024



ISO/IEC 17024



ISO/IEC 17024



ISO/IEC 17024



Credentials – The *Gold Standards* in information security certification

- Certified Information Systems Security Professional (CISSP)
- Certification and Accreditation Professional (CAP)
- Systems Security Certified Practitioner (SSCP)

CISSP Concentrations – In-depth, specialized enhancements to the CISSP

- Information Systems Security Architecture Professional (ISSAP)
- Information Systems Security Engineering Professional (ISSEP)
- Information Systems Security Management Professional (ISSMP)

Meant for professionals who:

- Are experienced professionals who manage and enforce information security policies
- Have minimum 5 years cumulative work experience in CBK® domains, or 4 years and applicable college degree
- Subscribe to (ISC)² Code of Ethics
- Are endorsed by another member of (ISC)²
- Pass a rigorous exam to assess their knowledge, skills and abilities relevant to the CBK
- Earn 120 hours of Continuing Professional Education (CPE) every 3 years for recertification
- May pursue specialized concentrations available in several areas of the CBK





CISSP CBK® Domains

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security





- Access Control Systems and Methodology
- Telecommunications and Network Security
- Cryptography
- Requirements Analysis and Security Standards/Guidelines Criteria
- Technology Related Business Continuity Planning (BCP) & Disaster recovery Planning (DRP) & Continuity of Operations Planning (COOP)
- Physical Security Integration





ISSEP® CBK Domains

- Systems Security Engineering
- Certification & Accreditation
- Technical Management
- U.S. Government Information Assurance (IA) Regulations





- Enterprise Security Management Practices
- Enterprise-Wide Systems Development Security
- Overseeing Compliance of Operations Security
- Understand Business Continuity Planning (BCP) & Disaster recovery Planning (DRP) & Continuity of Operations Planning (COOP)
- Law, Investigations, Forensics and Ethics

Certification and Accreditation Professional (CAP®)

Meant for professionals who:

- Formalize processes used to assess risk and established security requirements
- Ensure information systems possess security commensurate with the level of exposure to potential risk
- Possess at least 2 cumulative years of relevant certification and accreditation work experience
- Subscribe to the (ISC)² Code of Ethics
- Pass the CAP certification examination based on the requirements of knowledge, skills and abilities identified
- Earn 65 hours of CPE credits every 3 years



- Understanding the Purpose of Certification
- Initiation of the System Authorization Process
- Certification Phase
- Accreditation Phase
- Continuous Monitoring Phase





Systems Security Certified Practitioner (SSCP®)

Meant for professionals who:

- Are systems and network security administration professionals
- Possess a minimum 1 year cumulative professional experience in SSCP CBK® domains
- Subscribe to (ISC)² Code of Ethics
- Earn 60 hours of CPE credits every 3 years





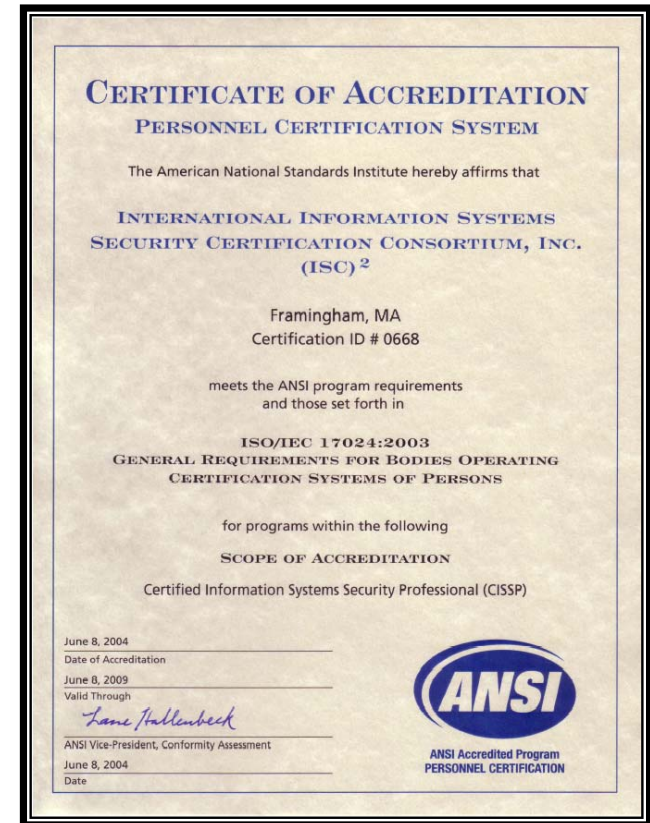
SSCP® CBK Domains

- Access Control
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware



Accreditation under ANSI/ISO/IEC Standard 17024

- **International Standards Organization** – Nearly 150 countries
- **American National Standards Institute** – US Representative to ISO
- **ANSI/ISO/IEC Standard 17024**
 - 88 countries participated
 - personnel certification system standard
- **(ISC)² CISSP, CISSP-ISSEP and SSCP Credentials**
 - Among 1st worldwide information security credentials to achieve accreditation under ANSI/ISO/IEC Standard 17024
- **Establishes global benchmark for assessing and certifying personnel**
- **A global standard benefits**
 - The information security profession
 - Businesses and governments
 - (ISC)² credential-holders





Associate of (ISC)²

- **Program to**

- Provide early support for information security careers
- Set new entrants on the right path early in their careers
- Encourage early commitment to the profession
- Accelerate the growth of professionals worldwide

- **Designed for candidates who**

- Pass the CISSP® or SSCP® examination
- Lack professional experience required for certification
- Are willing to subscribe to the (ISC)² Code of Ethics

- **Indicates a candidate**

- Possesses an independent and objective measure of competence via understanding of the (ISC)² CBK®
- Aspires to adhere to the rigors and ethics of the profession through association with (ISC)²
- Is required to complete the necessary professional experience and the subsequent endorsement process within 6 years

- **Provides access to suite of (ISC)² career support programs**

- Publications, research, CPE opportunities, peer networking, online forums





Educational Offerings

Voted “Best Professional Training Program” by SC Magazine in 2006 & 2007 and “Best Certification Program” in 2008

- **Providers of only (ISC)²-authorized CBK Review Seminars for CISSP, SSCP and CAP through (ISC)² Education and dozens of authorized academic affiliates around the world**
- **eLearning and instructor-led course options**
- **Annual (ISC)² Information Security Scholarship Program – US\$100,000**
- **Continuing education for (ISC)² certified members**
 - **(ISC)² Security Leadership Series**
 - **e-Symposia**
 - **Discounts to industry conferences held by many globally renowned providers**



Thoughts in the State of the IT Security Profession

- We have become a separate, distinct profession
- We are in a growth profession
- We are also well compensated
- It is becoming increasingly granular
- Many universities are adding IT security degree programs
- Certifications are increasingly important—both in the technical and non-technical areas
- DOD certification program may be implemented across the federal government
- State and local governments are the next major growth area

It's the People!



SECURITY TRANSCENDS TECHNOLOGYSM

SANS



SANS and GIAC in a Nutshell

May 2008

jpike@giac.org



What Is SANS/GIAC



- SANS Training
 - Leading training organization in system, audit, network, and security
 - Focused on intensive training
- GIAC Certification
 - Leading certification that validates the job based technical skills of security professionals



SANS/GIAC Guiding Principles

- **Education**

- Instructors from the trenches; winners of a multi-year competition for best teachers
- Current, Evolving Material
- Hands-on training
- Certification that validates your hard work

- **Community**

- Consensus from the community



Ways to Get SANS Training

- Live Training at SANS Conferences
- Local Mentor Program
- Instructor Led Online Training
- Self Study
- On-Site Classes
- OnDemand



University Style Course List

1. Discipline (SEC, AUD, MGT)

2. Level of Difficulty

300 – beginner

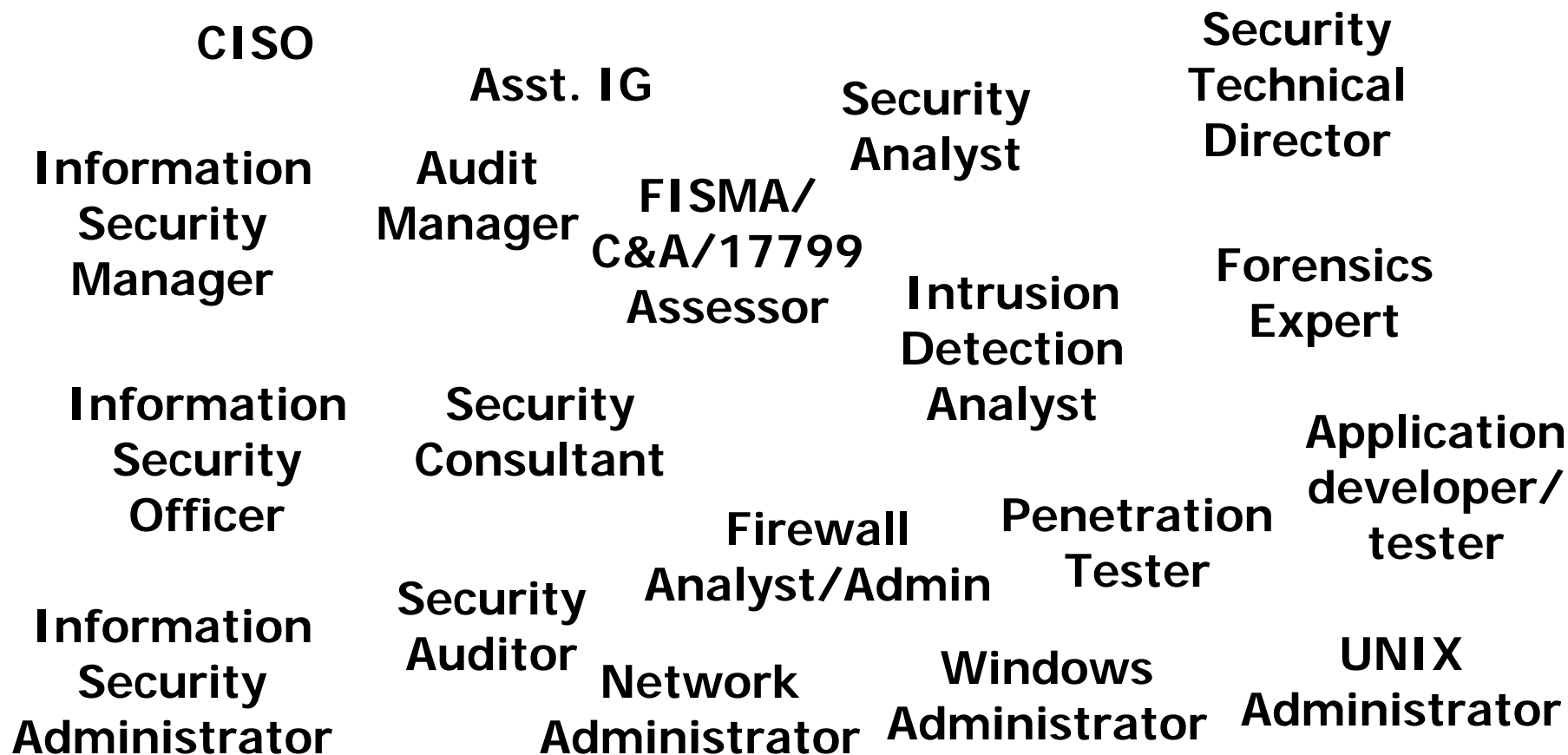
400 – some experience (either technical or ITSEC)

500 – advanced skills for experienced pros

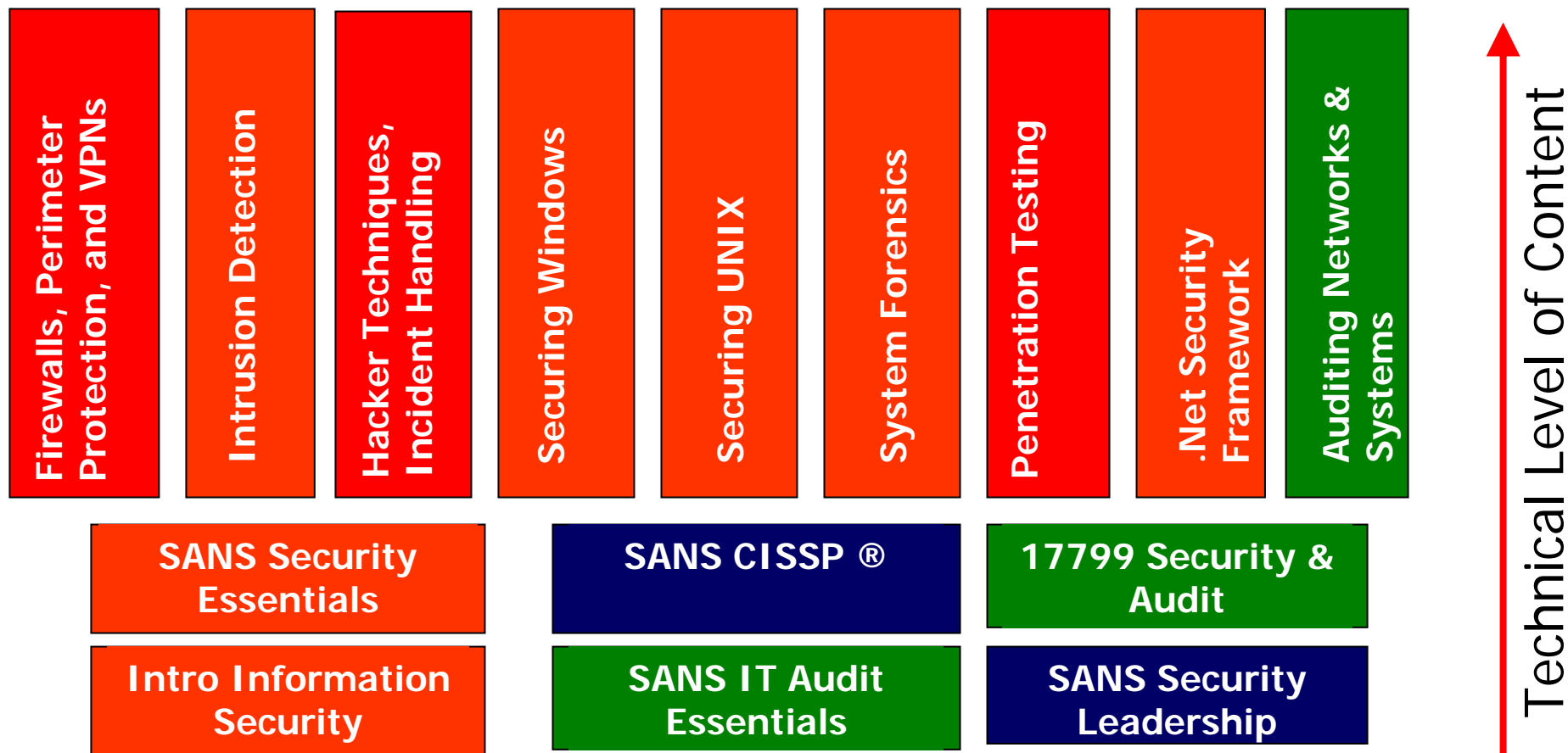
600 – even more advanced



What Are The Key IA Jobs?



SANS Highlight of Courses Offered





SANS Objectives

- Provide relevant education with content that can be put to work immediately
- Allow only full-time practitioners to teach
- Recruit the highest rated teachers in the country.
- In summary: relevant, highly technical and immediately useful material taught by superb teachers.
- Grew from 140 students in 1993 to over 20,000 in 2007.



Cooperative Research Programs Began in 1997

- Consensus Step-by-Step Guides
 - Windows NT
 - Solaris
 - Linux, etc.
- Roadmap to Network Security
- Security Policies Library
- Weekly Security Bulletins
- Security Flash Reports
- Y2K project for the White House
- Internet Storm Center



Expanded Research/ Public Policy Programs

- SANS Security Research Papers Collection
- Weekly Critical Vulnerability Alerts
- Common testing tools for security
- SANS/FBI Top Twenty Critical Vulnerabilities
- Worm Identification; White House Situation
- House and Senate Testimony
- Chaired House of Representatives Working Group on Use of Procurement to Improve Security



What is GIAC?

- GIAC is the 'Global Information Assurance Certification' program
- GIAC assesses candidate knowledge in specific subject areas and grants credentials in the field of IT Security
- GIAC's Certifications are specific to actual skill sets and job duties required in the IT Security industry.



Top 3 Reasons to Earn Your GIAC Certification

1. Hiring managers use GIAC certifications to ensure that candidates actually possess deep technical skills
2. GIAC certifications help IT Security Professionals get promoted faster and earn more money
3. GIAC candidates learn and absorb more of the detailed content through preparing for certification exams



GIAC Certifications

- GSEC - Security Essentials
- GCFW - Firewall Analyst
- GCIA - Intrusion Analyst
- GCIH - Incident Handler
- GCFA - Forensics Analyst
- GCUX - Unix Security
- GCWN - Windows Security
- GNET - . NET
- GSOC - Securing Oracle
- GSSP-JAVA - Secure Coding
- GSSP-C - Secure Coding
- GISF - Information Security Fundamentals
- GSAE - Security Audit Essentials
- GSLC - Security Leadership
- GSNA - System & Network Auditor
- G7799 - ISO 17799/27001
- GISP - Information Security Professional
- GCIM - Incident Manager
- GAWN - Auditing Wireless Networks
- GREM - Reverse-Engineering Malware
- GPEN - Penetration Tester
- GCPM - IT Project Management

For a complete list of GIAC Certifications
<http://www.giac.org/certifications/roadmap.php>

GIAC Certification



GIAC Silver Certifications

- Multiple choice exams only



GIAC Gold Certifications

- Plus a written technical report



GIAC Platinum Series

- Highest certification level



Proctored Exams

- ALL Certification exams are fully proctored
- Exams are open book, but not open computer
- Kryterion is GIAC's official partner for administering proctored exams
- A full list of Kryterion sites is available at:
<http://www.giac.org/proctor/kryterion.php>
- GIAC also offers other proctor options, if there is not a Kryterion site in your area. For more information on specific proctor requirements please visit <http://www.giac.org/proctor/>



Alternative Proctor Details

- GIAC offers proctored exams at many SANS conferences
- As a secondary option, it is also possible to take a proctored GIAC exam through your corporate human resources / training departments or local universities / colleges
- Non-Kryterion proctors will need to complete a GIAC proctor form and have it approved by GIAC prior to proctoring a GIAC exam
- This process can take a few days, so please plan in advance



ANSI Accredited Program
PERSONNEL CERTIFICATION

ISO/ANSI 17024 Accredited

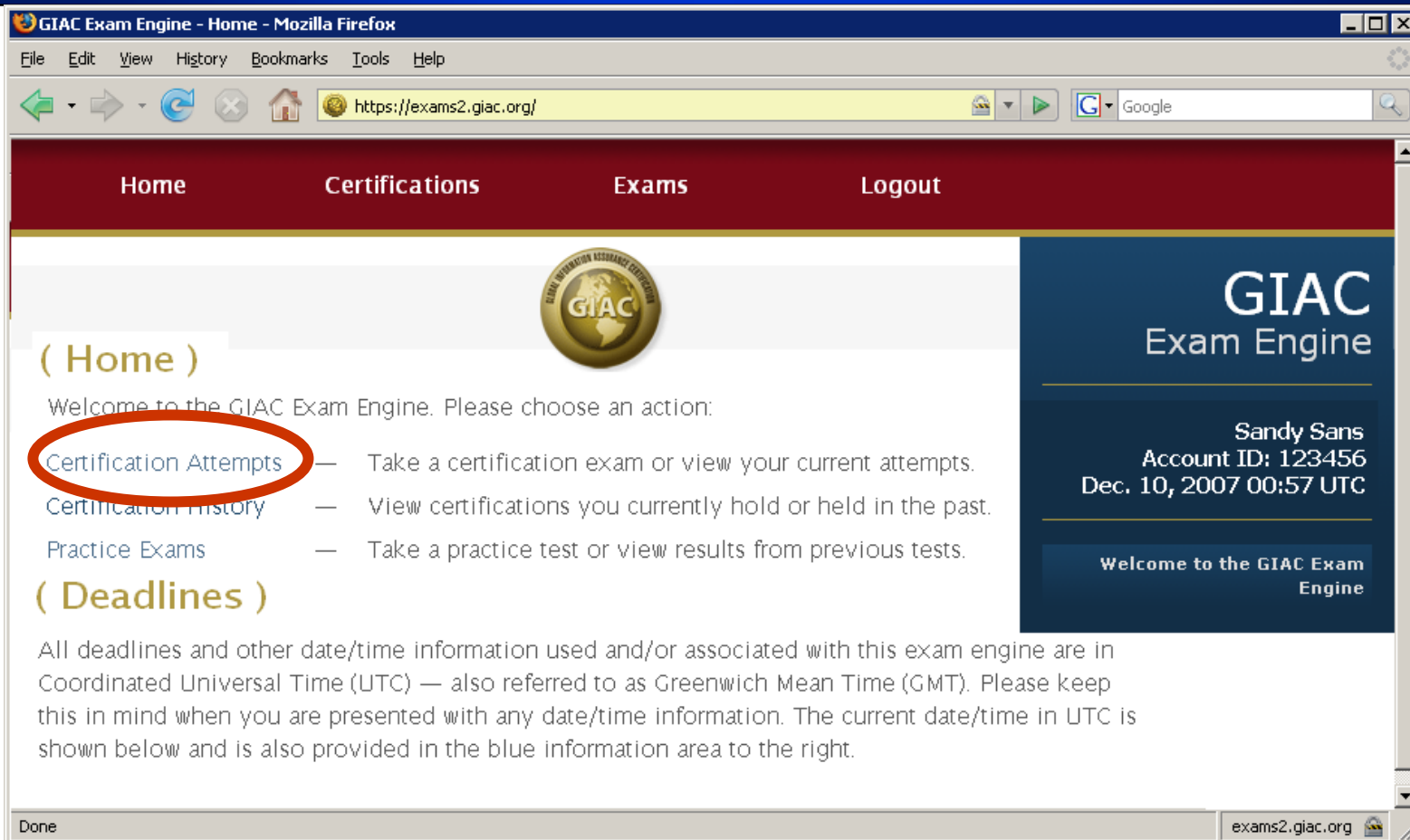
- ISO/ANSI 17024 is a quality standard for organizations granting certifications
- The GIAC certification program was accredited by the American National Standards Institute (ANSI) in December of 2007, under the ANSI/ISO/IEC 17024 standard
- This accreditation affirms and ensures GIAC operates a responsible, fair and quality oriented testing and certification granting organization



GIAC Exam Details

- ALL GIAC certification exams are taken online, in a proctored environment
- All material for a given Certification is covered in one exam
- Exams are open book and notes (think paper), not open electronic devices (no Google or pdfs)
- Most Certifications are 150 question, four hour exams (GSEC is 180 questions, five hour)
- You receive two practice tests
- Your certification exam must be completed **within 120 days** of account activation.

New GIAC Exam Engine




The screenshot shows a Mozilla Firefox browser window with the title "GIAC Exam Engine - Home - Mozilla Firefox". The address bar displays "https://exams2.giac.org/". The website has a dark red navigation bar with links for "Home", "Certifications", "Exams", and "Logout". Below the navigation bar, there is a circular GIAC logo. The main content area is divided into two columns. The left column contains a section titled "(Home)" with a welcome message and a list of actions: "Certification Attempts" (circled in red), "Certification History", and "Practice Exams". Below this is a section titled "(Deadlines)" with a paragraph of text. The right column features a dark blue sidebar with the text "GIAC Exam Engine", the user's name "Sandy Sans", account ID "123456", and login time "Dec. 10, 2007 00:57 UTC". At the bottom of the sidebar, it says "Welcome to the GIAC Exam Engine". The browser's status bar at the bottom shows "Done" and the URL "exams2.giac.org".

GIAC Exam Engine - Home - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://exams2.giac.org/

Home Certifications Exams Logout



(Home)

Welcome to the GIAC Exam Engine. Please choose an action:

- Certification Attempts** — Take a certification exam or view your current attempts.
- Certification History — View certifications you currently hold or held in the past.
- Practice Exams — Take a practice test or view results from previous tests.

(Deadlines)

All deadlines and other date/time information used and/or associated with this exam engine are in Coordinated Universal Time (UTC) — also referred to as Greenwich Mean Time (GMT). Please keep this in mind when you are presented with any date/time information. The current date/time in UTC is shown below and is also provided in the blue information area to the right.

GIAC
Exam Engine

Sandy Sans
Account ID: 123456
Dec. 10, 2007 00:57 UTC

Welcome to the GIAC Exam Engine

Done exams2.giac.org



Challenge Certifications

- Attempting GIAC Certification without training from SANS
- Same requirements apply
- Practice exams are provided
- Available for many certifications



Preparing for Your GIAC Exam

- Reread all the slides and notes sections from your course material
- Create a study index from your course material and your notes
- Listen to the course audio mp3 files
- Utilize your practice tests



Study Time

- On average, students who pass their GIAC exams put in 55 hours of study time, in addition to classroom training
- For GSEC the average is higher, over 70 hours
- Take time to prepare, it will pay off!



Certification Maintenance

- Security changes rapidly!
- Courseware is updated three times every year
- GIAC certifications are valid for four years
- \$325 to retest, 4 months to complete, includes current courseware from SANS
- Discounts available for multiple recertification attempts purchased in the same calendar year
 - After the first one, all others in same calendar year are \$200
- Benefits to recertification:
 - The longer you hold the certification, the more valuable it is
 - Retain your Gold status and original analyst number, option to update your paper

GIAC Identification

- GIAC offers many unique certifications
- Use the **GIAC** acronym as an identifier on business cards and resumes
- People will identify your individual certifications with the GIAC name





Advisory Board

- Open to anyone who earns an overall exam score of at least 90% when obtaining a GIAC certification
- Honors and demonstrated interest
- Opportunities
- Benefits
- Responsibilities



GIAC Alumni Linked In

- GIAC now has an 'Alumni Group' on the LinkedIn network
- If you are GIAC certified and part of the LinkedIn community, please use this link to be included
<http://www.linkedin.com/e/gis/38376/45794D211EFE>
- This helps fosters GIAC alumni communication outside of the conference setting
- LinkedIn profiles offer some geographical information, it is a way to stay connected with GIAC certified professionals in your general area



SANS Technology Institute

- GIAC is one of the assessment and grading arms of the SANS Technology Institute
- STI is a Masters degree program
- Two students have graduated
- Candidacy application is in place for accreditation
- Many students are currently enrolled
- Applications are being accepted
- <http://www.sans.edu> for more info



Thank you!

DSIA TRAINING OPPORTUNITIES

Jack Spooner

State Internal Auditor

May 21, 2008



Identification of Training Needs

- Survey Internal Audit Depts.
- Identify Areas of Interest
- Send Out 2nd Survey
- Solicit SWAM Vendors
- Solicit SWAM and Non-SWAM Vendors
- Prepare Contracts

Course Information

- How Many Classes are Offered?
- Where are They Offered?
- When are They Offered?
- How Long are the Classes?
- How Much Do They Cost?
- Are CPE Credits Earned?
- Who Teaches the Courses?
- Are Refreshments Provided?

Proposed Courses for FYE 2009

- Auditing with ACL
- MAP: The Managerial Assessment of Proficiency
- COSO-Based Auditing
- Critical Thinking+ Strategic Thinking= Problems Solved
- Using Data Mining to Detect Fraud & Errors
- Ethical Behavior and Professionalism
- Fraud Investigation for Government Auditors
- Interviewing Skills for Auditors
- Business Writing Solutions for Government Auditors
- One or Two Classes Yet To Be Determined

Registration Procedures

- Classes are Listed in July
- State Agency and Institution Internal Auditors Have First Choice
- State Employees and Others Register Through the DOA Website
- Attendees Are Invoiced Via IAT Vouchers or Bills
- For Registration Assistance, Call DSIA at 804-225-3106, ext. 23

Questions?



Altiris Security

Don Kendrick, Senior Manager of Security Operations, VITA

Rodney Caudle, Security Architect, NG

Jeff Grieger, Systems Architect, NG

May 21, 2008



NORTHROP GRUMMAN

QUESTIONS



Virginia Information Technologies Agency



IT System Security Guideline

ITRM SEC 515-00

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer

May 21, 2008





Topics Covered in the Guideline

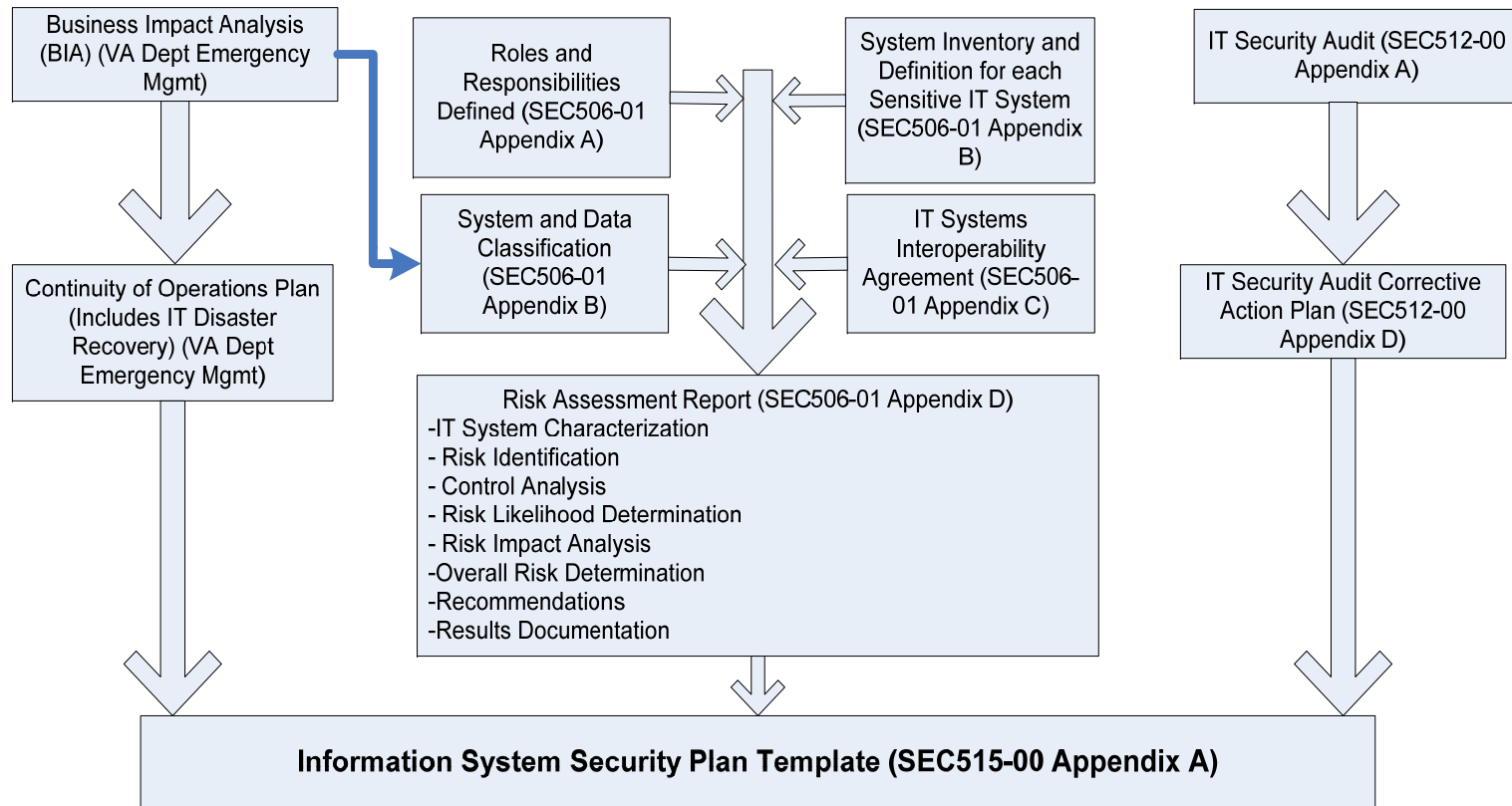
- IT Systems Security Plans
- IT System Hardening
- Malicious Code Protection
- IT Systems Development Life Cycle



IT Systems Security Plans

- Requirement of the Policy-Section 3.1.3 and the Standard-Section 4.2
- Provides a summary of the security requirements for the information system
- Describes controls in place or planned for meeting security requirements
- Existing security-related documents are used as input

IT Systems Security Plans





IT Systems Security Plans

Information System Security Plan Template

1. Information System Name/Title:

- Unique identifier and name given to the system.

2. Information System Owner and other Designated Contacts:

- Name, title, agency, address, email address, and phone number of person who owns the system along with others i.e. business owner, data owner, system administrator, ISO, etc .

3. Authorizing Official:

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.



IT Systems Security Plans

4. Information System Operational Status:

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

Operational	Under Development	Major Modification
-------------	-------------------	--------------------

5. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

6. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.



IT Systems Security Plans

7. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

8. Plan to Implement Recommended Controls (reference Risk Assessment)

- Provide a description of how security controls recommended from the risk assessment are being implemented or planned to be implemented, and who is responsible for the implementation.

9. Information System Security Plan Completion Date: _____

- Enter the completion date of the plan.



IT Systems Security Plans

Completion and Approval Dates

Agency Head or designated ISO approves the System Security Plan.

10. Information System Security Plan Approval Date:

-
- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.



IT Systems Security Plans

Ongoing System Security Plan Maintenance

- Review and update at least every three years or more often if necessary.
- Some items to include in the review are:
 - Change in information system owner;
 - Change in information security representative;
 - Change in system architecture;
 - Change in system status;
 - Additions/deletions of system interconnections;
 - Change in system scope;
 - Change in authorizing official.



IT System Hardening

- Baseline IT Security Configuration Standards
 - NIST (National Institute of Standards & Technology)
 - CIS (Center for Internet Security)
- Baseline IT Security Configuration Standards Records
- Vulnerability Scanning
- Baseline Review and Modification

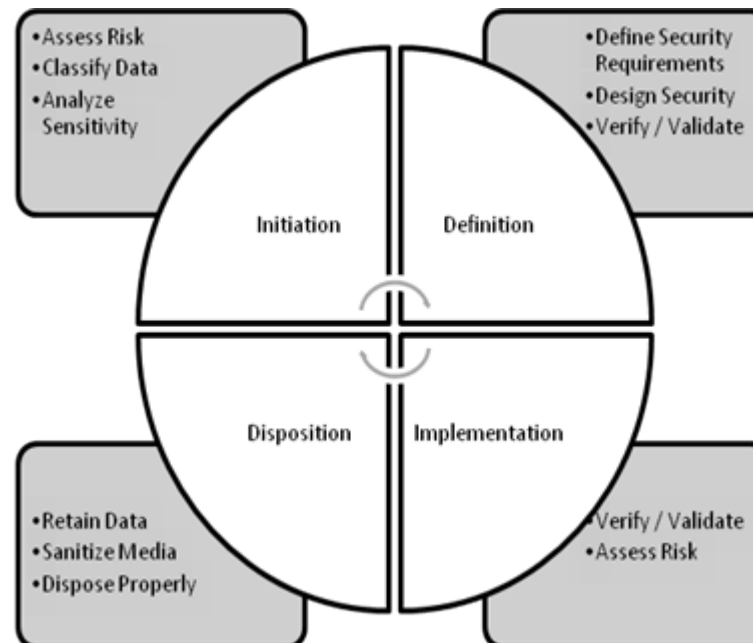


Malicious Code Protection

- Types of Malicious Code
 - Viruses and Worms
 - Trojan Horses
 - Rootkits
 - Spyware and Adware
 - Bots
- Malicious Code Protection Best Practices
 - Educate the users
 - Use multiple vendors for protection solutions
 - Centrally manage and update protection software
 - Use defense-in-depth approach
 - Hardware based malware protection solutions on the network edges
 - Malware protection solutions on each system

IT Systems Development Life Cycle

- Defines security-related tasks that must occur in each phase of a system's life cycle



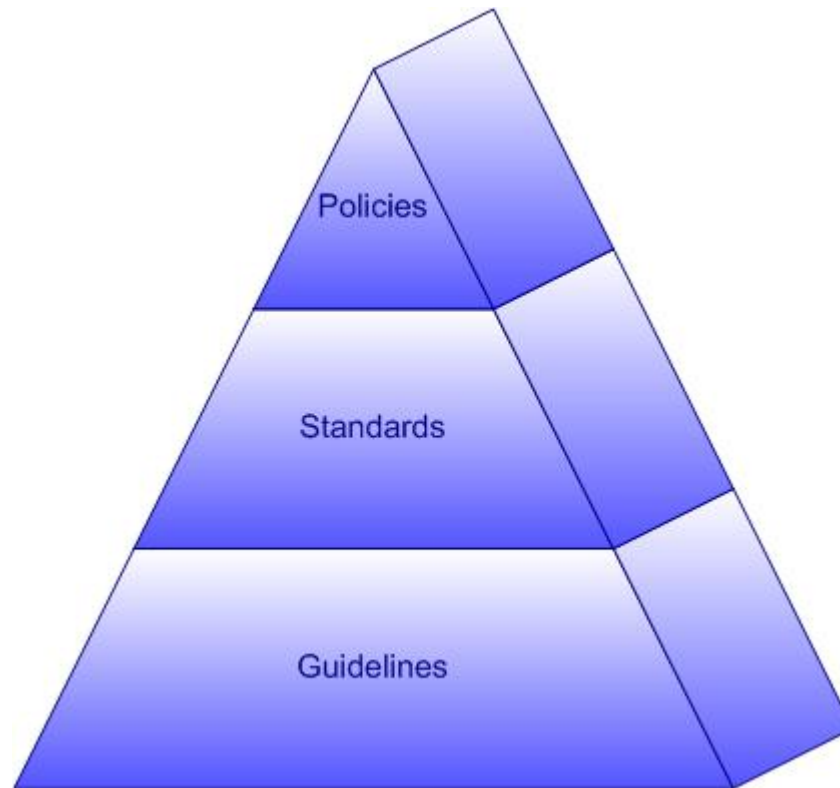


Summary

- IT Systems Security Guideline (ITRM SEC515-00) is on ORCA until June 10.
<https://apps.vita.virginia.gov/publicORCA/default.asp>
- Compliance date for IT Systems Security Plans for sensitive systems is July 1.



Questions and/or Comments?



Thank you!



Virginia Information Technologies Agency



Email Encryption

Michael Watson

Incident Management Director

ISOAG Meeting

May 21, 2008





Why do we use Email Encryption?

- Email Encryption Enables 2 Primary Functions
 - Secure Email – Encrypted Mail
 - Email is protected from unauthorized parties viewing the data
 - Identity Confirmation – Digital Signatures
 - Verification that the email is from the person in the senders/from field.



Establishing Your Identity

- You need to be who you say you are...
 - Establish your identity with a digital representation.
 - Private Key
- You need others to know if you have changed who you are...
 - If you must change your digital identity there has to be a way to let people know.
 - Certificate Revocation List
- You need a way for others to confirm they have the right identity for you.
 - Confirmation that the digital representation hasn't been tampered with and is the one that belongs to you.
 - Fingerprint/Hash



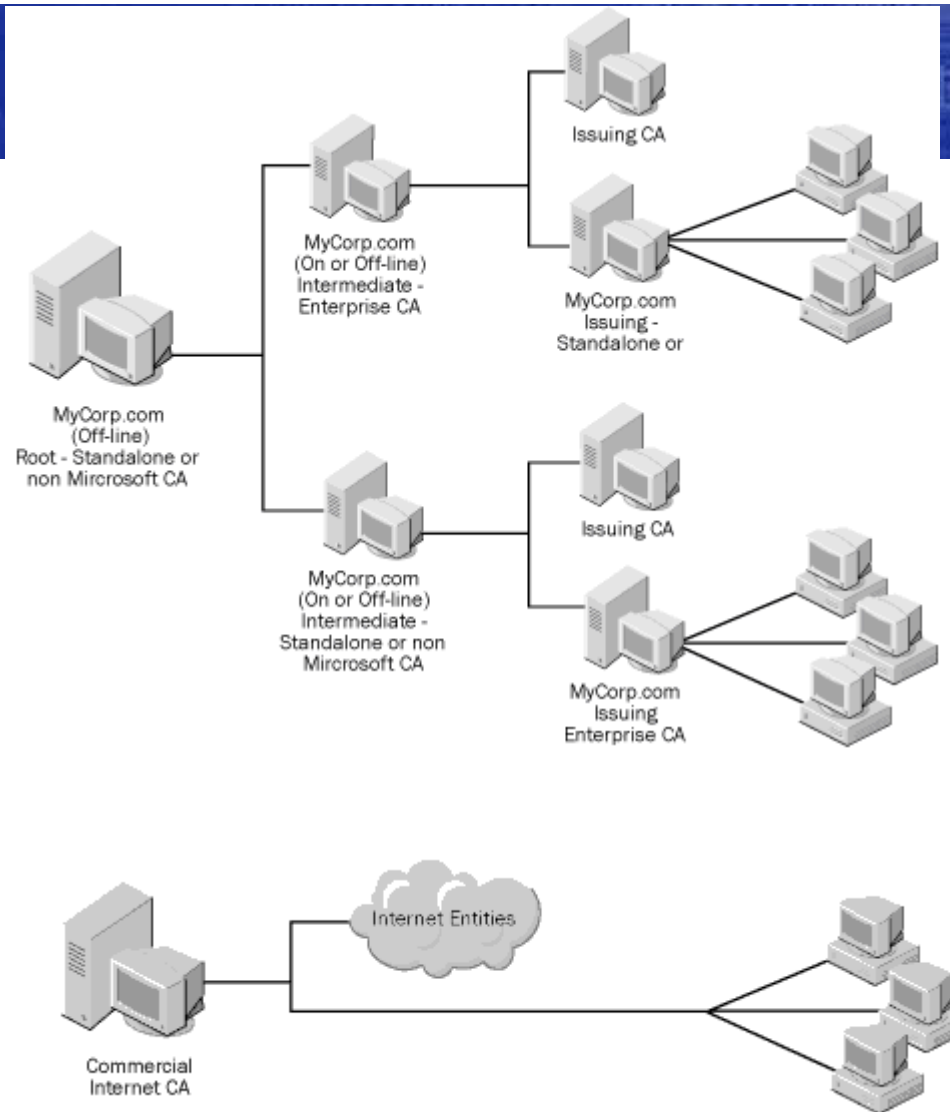
Establishing Others Identity

- You need to know that someone is who they say they are...
 - Verify their digital representation of themselves.
 - Verify their public key
- You need to know if someone changed who they said they were...
 - If you must change your digital identity there has to be a way to let people know.
 - Certificate Revocation List
- You need a way to confirm that they have what you originally sent.
 - Confirmation that the digital representation hasn't been tampered with and is the one that belongs to them.
 - Fingerprint/Hash



Trusting the Identity

- Establishing Trust
 - Certificate Authority (CA) – The entity that issues certificates.
 - If trusted all certificates from this CA are also trusted.
 - CA's have their own certificates.
 - The CA becomes trusted by “installing” the CA certificate
 - Certificate Revocation List (CRL) – A list of certificates that should not be trusted.
 - When a certificate is compromised.
 - Fingerprint – A hash of a certificate.
 - Use the fingerprint to confirm that the certificate belongs to the user.





The Trust Runs Out – Key Management

- Revoking Certificates
 - Compromise, Loss, Exposure, etc.
 - Certificate Revocation Lists
- Previous encrypted data may be lost
- Enterprise Management
 - How do administrators monitor encrypted data?
 - Must have access to private key
- Key management must integrate into policies and procedures.
- Expiring Trust
 - Keys, like passwords, can expire after a period of time.



Basic Cryptography

- Cryptography allows the exchange of information to remain private between parties.
- Two primary forms of cryptography
 - Asymmetric Encryption
 - 2 keys – Public and Private
 - PKI, Diffie-Helman, RSA
 - Symmetric Encryption
 - 1 key – Secret Key
 - AES/Rijndael, 3DES, DES, Blowfish
- Often protocols employ both when encrypting data
 - SSL, TLS, IPSEC



The Importance of Hashes

- Hash – Unique representation of a set of data.
- 3 Important Properties
 - Preimage Resistance
 - One Way to Compute
 - Second Preimage Resistance
 - Hard to guess the input that results in the unique output
 - Collision Resistance
 - Two different inputs shouldn't equal the same output
- Hashes are used to compute fingerprints of data
 - Summarize data (digest)
 - MD5, SHA-1, SHA-2, and coming soon: SHA-3



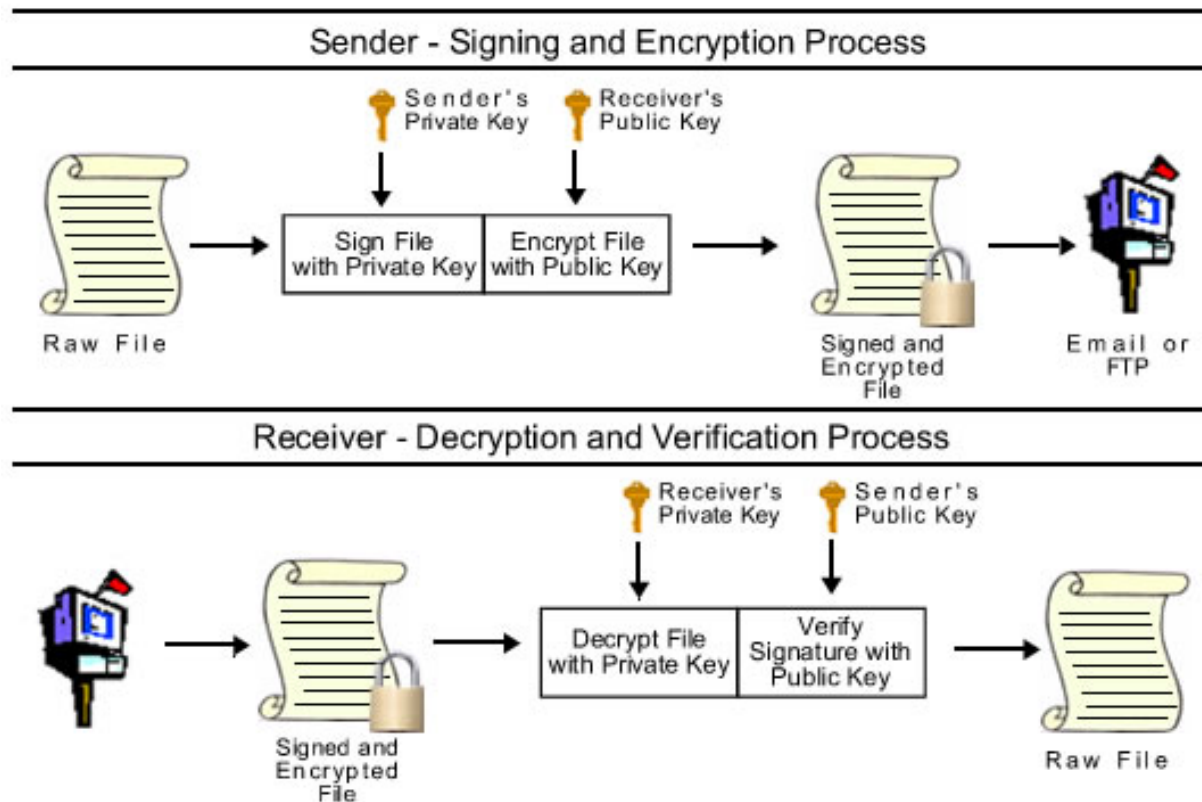
Why is this cryptography stuff important?

- Designated partnership email encryption solution
 - Asymmetric Encryption
 - AKA Public/Private Key Encryption
 - Digital Signatures
- S/MIME
 - standard for public key encryption and signing of e-mail encapsulated in MIME (email messages)
 - Provides authentication, message integrity and non-repudiation of origin (digital signatures) and data security via encryption.



How can I make this work for me?

- Trust
 - In order for certificates/keys to work properly the Certificate Authority for the certificate issuer must be trusted.
- Sending an email to another person
 - The sender (you) must have the recipients' ("them") public key.
- Receiving an email from someone
 - The sender ("them") must have your public key.
- Verifying a digital signature
 - The receiver (you) must have the senders' ("them") public key.
- If multiple parties are receiving email the sender must have all of the recipients public keys.





Understanding the Risks of Encryption

- What happens when a certificate is revoked or destroyed?
 - Email history
- Monitoring of Encrypted Mail
- Ensuring all communication is encrypted
- Agency management of a certificate
- Who possesses the certificate?



The Partnership Solution

- Partnership manages the certificate issuance
 - Installation
 - Distribution
 - Revocation Lists
- Agency manages the authorization of certificates
 - Approves certificate issuance
 - Establishes policy for certificate usage
 - Includes ensuring compliance
 - Decides when to revoke a certificate



Questions?

Thank you!



QUESTIONS?





Virginia Information Technologies Agency



Upcoming Events





UPCOMING EVENTS

IS Orientation

Wednesday, May 29th, 1 to 3:30 pm @ CESC
and **Monday, June 23rd**, 2 to 4:30 pm @ CESC

IS Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email VITASecurityService@VITA.Virginia.gov



UPCOMING EVENTS

Commonwealth Information Security Council Meeting

Monday, June 16, 12:00 - 2:00 p.m. @ CESC with
Committee meetings from 2:00 - 3:30 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to VITASecurityServices@vita.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at

<http://www.vita.virginia.gov/security/default.aspx?id=5128>



UPCOMING EVENTS!

FREE GARTNER LOCAL RISK, SECURITY & COMPLIANCE BRIEFING

Tuesday, June 17 from 8:00 am to 11:15 am **Roberta Witty** Research VP,
Gartner <<http://www.gartner.com/AnalystBiography?authorId=14667>>

Risk, Security & Compliance

Register Today

<<http://www.gartnerinfo.com/lbsec061708/index.php?e=94907886ebba7f4c438e40af99ec67f9l76804515>>

Where: Richmond Marriott

<<http://www.marriott.com/hotels/travel/ricdt-richmond-marriott/>>

500 East Broad Street

Richmond, Virginia 23219

Phone: 804-643-3400



UPCOMING EVENTS!

NEXT ISOAG MEETING!

June 18 1:00 – 4:00

@ CESC



Virginia Information Technologies Agency



Any Other Business ??????



ADJOURN

THANK YOU FOR ATTENDING!!

